enterprise privacy office

Data Lifecycle Management

PPU-2017-03

» Data must be managed and protected throughout its lifecycle. The data lifecycle spans from the point of collection or creation to the action of disposal. Your organization must take appropriate steps to reduce privacy risks at each stage of the data lifecycle.

CREATE/COLLECT

- Information is created and collected in a multitude of formats, using various methods and technologies. New information collected by the organization should be inventoried and classified in writing.
- A key principle during this phase is to collect only the minimum information needed to perform the business function. Be sure to follow your agency's policies and procedures on creating, collecting and capturing data.

STORE

- Considerable analysis should go into determining the right environment for information storage. If information is stored electronically, information technology and security teams must be consulted to establish the best safeguards. Physical environments, such as secure physical spaces and storage containers, must be assessed prior to paper document storage. Also keep in mind that your organization may want to completely avoid storing certain information on portable storage devices, such as thumb drives and DVD/CDs.

USE

- Information should be accessed, transmitted, or manipulated by only authorized users conducting official business. Carefully review criteria and procedures for access privileges.

SHARE

- The organization does not absolve itself of the responsibility to protect information collected, when it shares that information with other entities.
- Written agreements and contracts must be established with third parties to set requirements regarding information protection, use limitations and incident reporting.

ARCHIVE

- Over time, the value of data may change. For example, certain information changes frequently and is more likely to become invalid as it ages. Other information may need to be transferred from active storage to archives because the need for access has decreased.
- Do not retain information longer than is necessary to accomplish your business processes. Be sure to follow your agency's guidance and procedures on data retention schedules.

DISPOSE

- When information reaches the end of its required retention period, it may be destroyed or preserved permanently in an archive for on-going historical reference or research purposes.
- Disposal methods vary based on the sensitivity of the information, so check your agency's policies and procedures.

PRIVACY POWER-UP

WHAT ARE PRIVACY POWER-UPS?

- Tips to ***ENERGIZE*** privacy program Implementation.
- Pointers on information privacy safeguards, training techniques, and compliance activities.
- Synopses of privacy hot topics, research, and technologies.
- Tools for agency privacy liaisons to increase privacy awareness and establish information privacy protections.

admin
THE SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION